Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

REPLY COMMENTS

CenturyLink Public Communications, Inc. ("CenturyLink") submits these Reply Comments pursuant to the Commission's Report and Order and Further Notice of Proposed Rulemaking released in this docket on March 24, 2017 (the "*Notice*").[1]

I. INTRODUCTION

CenturyLink is a provider of inmate calling services ("ICS") to correctional institutions throughout the United States. CenturyLink serves both jails and prisons, both urban and rural, but is most concentrated in the prison market. As an ICS provider, CenturyLink is very aware of the well-documented danger of contraband cell phones in correctional facilities. Inmates have used contraband cell phones to threaten witnesses and victims, run smuggling and drug operations, and commit fraud and a wide variety of other crimes – even order the murders of judges, prosecutors and witnesses.

Correctional facilities are increasingly requiring ICS providers such as CenturyLink to bundle "value-added" services such as Contraband Interdiction Systems ("CIS") into ICS procurements in order to address the problem of contraband cell phones. Among correctional facilities, prisons have been most interested in CIS thus far. As a result, CenturyLink has

[1] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336 (2017); 82 Fed. Reg. 22780 (May 18, 2017).

firsthand experience with several types of CIS including portable detection devices, antenna-based detection technologies, and Managed Access Systems ("MAS").

In addressing the serious problem of contraband cell phones, and the dangers they represent to public safety and correctional personnel, CenturyLink's correctional institution customers have expressed a strong preference for automated controls. Manual search and seizure of contraband cell phones is extremely challenging – and in some cases impossible – for correctional institutions to effectively conduct. Tight budgets and the inherent danger of correctional work together create chronic and sometimes severe understaffing. Putting officers into situations where they must manually seize contraband cell phones in close contact with potentially dangerous inmates, often with short-staffed backup, greatly increases that danger.

CenturyLink agrees with those commenters who have advocated that the Commission adopt rules that allow for a variety of solutions to address the problem of contraband cell phones.[2] To date, MAS has been the default alternative for detection and automated control of contraband devices. However, as several commenters pointed out, MAS has a number of well-documented limitations, including very high cost.[3] CenturyLink believes that Denial of Service ("DoS") technologies present the best balance of technological efficacy, operational manageability, and cost efficiency for many correctional facilities. Accordingly, the Commission should adopt rules that facilitate the deployment of these technologies among others.

[2] *See, e.g.*, Comments of Global Tel*Link Corporation, filed June 19, 2017, pp. 2-3.

[3] *Id.*, at p. 3; Comments of American Correctional Association, filed June 19, 2017, pp. 2, 4-5; Comments of the Tennessee Department of Correction, filed June 19, 2017, p. 5; Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking, filed June 19, 2017, pp. 7-10.

II. THE COMMISSION SHOULD ADOPT RULES TO FACILITATE THE DEPLOYMENT OF DoS TECHNOLOGIES

One type of CIS system that the Commission should facilitate is technology that allows a correctional facility to detect and identify contraband cell phones. Once identified, the correctional facility can request wireless carriers to discontinue service or otherwise disable the use of the illegal cell phones. CenturyLink refers to this type of CIS as "Denial of Service" or "DoS". DoS requires equipment that can detect and identify contraband cell phones and a way for correctional facilities to compel wireless carriers to terminate service to, or otherwise disable, the cell phones.

Some commenters have noted that DoS is not a perfect solution to contraband cell phones. They have cited such issues as the lack of control for non-cellular technologies such as Wi-Fi.[4] Nevertheless, DoS is a leading solution to the problem of contraband cell phones and has a number of attractive features.

First, DoS requires only moderate coordination between detection systems and wireless carriers. Second, it is highly effective to the extent that the subscriber account is permanently disabled, preventing all future communication attempts. Third, it is much more cost effective than MAS. DoS does not require the very expensive MAS control radios, which must be separately implemented for each carrier and protocol, constantly tuned for changes in the RF environment, and upgraded – often with a substantial time lag – as technology changes.

To enable the deployment of DoS technologies, the Commission should adopt reasonable rules requiring wireless carriers to either terminate service to a contraband cell phone or otherwise disable the device upon receipt of a qualified request from a correctional facility. The

[4] *See, e.g.*, Cell Command, Inc.'s Comments, pp. 13-15.

Commission's rules should define what constitutes a qualified request to terminate service or disable a wireless device and who qualifies as an authorized party to make such a request.

CenturyLink agrees with CTIA that a qualifying request should include a device's International Mobile Subscriber Identity ("IMSI"), as well as the correctional facility in which the device is operating.[5] This information should allow a wireless provider to accurately prevent use of the unauthorized device on its network. CenturyLink agrees with AT&T that the party authorized to make a request to terminate service or disable a wireless device should be someone with the authority and incentive to ensure that a list of identified contraband devices is correct.[6] Authorized parties should include senior corrections officials, including officials of privately run facilities.

CenturyLink disagrees with those commenters who propose that a court order process be required before a wireless carrier is allowed to terminate service or disable a wireless device. A system that requires a correctional institution to apply to a court of competent jurisdiction to seek an order requiring a wireless carrier to discontinue service or disable an illegally operated wireless device is not required by law and will plainly be too slow and cumbersome.[7] As noted by Arizona Department of Corrections, "[t]he speed in which wireless devices are moved in prison would surprise people unfamiliar with corrections."[8] The public interest requires a more expeditious process and one that does not unnecessarily burden the resources of correctional facilities. Commission rules defining a qualifying request and identifying who is authorized to

[5] Comments of CTIA, filed June 19, 2017, p. 6.

[6] Comments of AT&T Services, Inc., filed June 19, 2017, p. 15.

[7] Comments of CoreCivic, filed June 16, 2017, p. 2.

[8] Comments of Arizona Department of Corrections, filed April 18, 2017, p. 2.

make such requests would provide sufficient protection against the risk that those lawfully using wireless devices will have their service terminated or devices disabled.

Wireless carriers have asserted that the Commission should review and certify detection systems used by correctional facilities to detect and identify contraband cell phones. They have expressed concern about the ability of detection systems to accurately identify contraband devices.[9] However, these commenters have not proposed specific certification standards that detection systems would have to meet, which makes it difficult to evaluate such a proposal. It is incumbent upon them to provide this information. Wireless providers have unique knowledge of their networks and customer bases and are thus uniquely positioned to know what specific certification standards are sufficient to ensure that service to legitimate wireless customers is not disabled.

Wireless carriers have also asserted that qualifying requests should be submitted through secure transmission paths such as secure web portals.[10] This is a reasonable and technologically feasible assertion, but here again, wireless carriers need to provide the specific details they would reasonably require and the specific format and submission process they would recommend before being directed to terminate service to a contraband cell phone. In addressing this very serious public safety issue, wireless carriers need to provide more information on the specific format and submission process than they have provided in their comments.

Admittedly, more information is also needed from CIS providers. CIS providers need to be very specific about what information they require from wireless providers concerning changes to their networks for CIS technologies to work properly. The CIS providers also need to

[9] *Notice*, 32 FCC Rcd at 2370 ¶ 90.

[10] *Id.*

describe exactly what information they can provide to wireless carriers to facilitate discontinuance of service to contraband cell phones. Without these details it again becomes difficult to evaluate these CIS technologies.

III. THE COMMISSION SHOULD GIVE FURTHER CONSIDERATION TO PRECISION JAMMING AND OTHER TECHNOLOGIES

The initial comments filed in response to the *Notice* addressed several other technologies besides MAS and DoS that merit further consideration, but the comments did not address all of them. For example, Precision Jamming is a technology that could be implemented today, and in many cases it may be a cost-effective and operationally effective solution to contraband cell phones.[11] Precision Jamming involves use of a radio signal jamming device to transmit on the same radio frequencies as wireless devices and base stations to disrupt the communication link between the illegally-operated device and the network base station, rendering any wireless device operating on those frequencies unusable.[12] Precision Jamming may work particularly well in rural areas where there is little risk of interference with legitimate wireless signals. The risk of interference with legitimate wireless signals may pose a more difficult problem in urban areas.

In its *2013 NPRM*, the Commission recognized that Section 333 of the Communications Act of 1934, 47 U.S.C. § 333, prohibits any person from willfully interfering with radio communications of any station license authorized under the Act or operated by the U.S. Government.[13] The Commission further noted that because radio signal jammers are used to

[11] Comments of the Tennessee Department of Correction, pp. 2-3.

[12] Notice of Proposed Rulemaking, *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, 28 FCC Rcd 6603, 6614 ¶ 18 (2013).

[13] *Id*., at ¶ 19 & n. 73.

willfully interfere with radio communications of licensed or authorized stations, jammers are not permitted under the Commission's rules, based on its current interpretation of Section 333.[14]

Several petitioners including the South Carolina Department of Corrections ("SCDC") had filed petitions requesting authorization to use Precision Jamming to prevent the use of wireless devices in correctional facilities, with appropriate safeguards to prevent interference with legitimate wireless communications. The SCDC asserted in its petition for rulemaking that those opposing Precision Jamming have read Section 333 of the Act too broadly and that reasonable rules allowing state and local correctional authorities to use precision jamming of illegally operated devices are possible and not prohibited by a more reasonable and modern interpretation of Section 333.[15] The Commission should give further consideration to, and seek additional comment on, the issues raised in SCDC's petition for rulemaking.

Some commenters have advocated that the Commission take steps to facilitate beacon technologies that render a wireless device incapable of use within correctional facilities. Beacon technologies rely on a system of beacons creating a restricted zone in a correctional facility, such that any wireless device in the zone will not operate.[16] Beacon technologies have a number of theoretical strengths, but as noted by several commenters, would require a lengthy process to establish standards for wireless devices and for numerous device manufacturers to develop the

[14] *Id*., at ¶ 19.

[15] Petition for Rulemaking of South Carolina Department of Corrections, filed August 6, 2009, *Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users; CellAntenna Corp. Request for Special Temporary Authority for Demonstration of Equipment to Block Wireless Calls by Inmates at Pine Prairie Correctional Center*, RM No. ___, WT Docket No. 09-30, pp. 7-11.

[16] *Notice*, 32 FCC Rcd at 2382 ¶ 130.

necessary hardware and software.[17] While beacon technologies cannot be implemented immediately, CenturyLink agrees that it is an alternative that should be explored further.

Quiet zones have similar theoretical strengths to beacon technologies, but they are operationally very complex and would require wireless providers to incur significant costs to develop software and re-engineer their networks.[18] Nonetheless, CenturyLink agrees with those commenters who advocate that this alternative be investigated further as well.

IV. CONCLUSION

In summary, and for the foregoing reasons, CenturyLink urges the Commission to adopt rules that allow for a variety of solutions to address the problem of contraband cell phones. These solutions should include, but not be limited to, Denial of Service technologies.

Respectfully submitted,

By: /s/ Thomas Dethlefs

Thomas Dethlefs
Suite 250
1099 New York Avenue, N.W.
Washington, DC 20001
(303) 992-5791

CENTURYLINK

Its Attorney

July 17, 2017

[17] *See, e.g.*, Comments of CTIA, pp. 9-10.

[18] *See, e.g.*, Comments of T-Mobile USA, Inc., filed June 19, 2017, pp. 3, 16.